Cryptography I, homework sheet 6

Due: 12 November 2010, 10:45

1. Let K be a field of characteristic p, where p is prime. Show that for any integer $n \geq 0$ one has
$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$
for all $a, b \in K$.
Hint: You can use the binomial theorem.

2. State all generators of $\mathbb{F}_5^*$ and of $\mathbb{F}_7^*$.

3. Let $f \in K[x]$ be a polynomial. Show that if α is a multiple root of f then $(x-\alpha) | \gcd(f, f')$.